Příručka správy osobního počítače

Stolní počítače pro obchodní účely

Číslo dokumentu: 312947-222

září 2003

Tato příručka obsahuje definice a pokyny k použití funkcí zabezpečení a strategie Intelligent Manageability, které jsou u vybraných modelů předem nainstalovány.

VAROVÁNÍ: Text označený tímto symbolem informuje, že nerespektování uvedených pokynů může vést ke zranění nebo k ohrožení života.

UPOZORNĚNÍ: Text označený tímto symbolem informuje, že nerespektování uvedených pokynů může vést k poškození zařízení nebo ke ztrátě dat.

Příručka správy osobního počítače
Stolní počítače pro obchodní účely

Druhé vydání (září 2003)
Číslo dokumentu: 312947-222

Obsah

Příručka správy osobního počítače

Rejstřík

Příručka správy osobního počítače

Strategie HP Intelligent Manageability nabízí standardní řešení pro správu a řízení stolních počítačů, pracovních stanic a notebooků v síťovém prostředí. Společnost HP se stala průkopníkem v oblasti správy stolních počítačů v roce 1995, kdy zavedla první stolní osobní počítače umožňující úplnou správu. Společnost HP je držitelem patentu na tuto technologii. Od té doby stojí společnost HP v čele vývoje průmyslových standardů a infrastruktur potřebných k efektivnímu zavádění, konfiguraci a správě stolních počítačů, pracovních stanic a notebooků. Společnost HP úzce spolupracuje s předními výrobci softwaru pro správu s cílem zajistit kompatibilitu strategie Intelligent Manageability s těmito produkty. Strategie Intelligent Manageability tvoří významný aspekt našeho jasného závazku poskytovat uživatelům produkty pro životní cyklus počítače, které uživatelům pomáhají v průběhu čtyř fází tohoto cyklu. Mezi tyto fáze patří plánování, zavedení, správa a přechodné fáze.

Klíčové schopnosti a funkce správy stolních počítačů jsou následující:

- počáteční konfigurace a zavedení,
- vzdálená instalace systému,
- aktualizace a správa softwaru,
- použití paměti ROM typu flash,
- evidence inventárních čísel a zabezpečení,
- zobrazení informací o selhání systému a jeho obnovení.

Podpora konkrétních funkcí popsaných v této příručce se může lišit v závislosti na modelu nebo verzi softwaru.

Počáteční konfigurace a zavedení

Počítač je dodán s předem instalovanou bitovou kopií (snímkem) systémového softwaru. Po krátkém procesu rozdělení softwaru na jednotlivé aplikace je počítač připraven k použití.

Je možné, že předem instalovanou bitovou kopii softwaru budete chtít nahradit vlastní sadou systémového softwaru s aplikacemi. Existuje několik metod zavedení vlastní bitové kopie softwaru. Mezi ně patří:

- instalace dalších softwarových aplikací po rozdělení předem instalované bitové kopie softwaru na jednotlivé aplikace,
- použití nástrojů pro zavedení softwaru, jako například Altiris Deployment Solution™, k nahrazení předem nainstalovaného softwaru vlastní bitovou kopií softwaru,
- použití procesu kopírování disků ke kopírování obsahu jednoho pevného disku na druhý.

Optimální metoda zavedení závisí na používaném prostředí a procesech informačních technologií. Informace, které vám pomohou při výběru nejlepší metody zavedení, najdete v části PC Deployment (Zavedení počítače) na webovém serveru HP Lifecycle Solutions (Řešení společnosti HP pro životní cykly) (http://h18000.www1.hp.com/solutions/pcsolutions).

Instalace založená na disku CD-ROM *Restore Plus!* a hardware s rozhraním ACPI poskytují další pomoc při obnově systémového softwaru, správě konfigurace, odstraňování potíží a řízení spotřeby.

Vzdálená instalace systému

Vzdálená instalace systému umožňuje spouštět a nastavovat systém pomocí informací o konfiguraci a softwaru umístěných na síťovém serveru, a to pomocí prostředí PXE (Preboot Execution Environment). Funkce vzdálené instalace systému obvykle slouží jako nástroj pro nastavení a konfiguraci systému a lze ji použít pro následující úlohy:

- formátování pevného disku,
- zavedení softwaru v jednom nebo více nových počítačích,
- vzdálená aktualizace systému BIOS v paměti ROM typu flash („Vzdálená paměť ROM typu flash na stránce 8“),
- konfigurace nastavení systému BIOS.

Chcete-li spustit vzdálenou instalaci systému, stiskněte klávesu **F12** poté, co se v pravém dolním rohu obrazovky s logem společnosti HP zobrazí zpráva F12 = Network Service Boot (F12 = Spuštění ze sítě). Dále postupujte podle pokynů na obrazovce. Výchozí pořadí spouštění je nastavení konfigurace systému BIOS, které lze změnit tak, aby vždy docházelo k pokusu o spuštění pomocí prostředí PXE.

Společnosti HP a Altiris, Inc. uzavřely partnerství s cílem poskytovat nástroje, které usnadní zavedení a správu podnikových počítačů, sníží časovou náročnost těchto procesů, podstatně sníží celkové náklady na vlastnictví a učiní z počítačů společnosti HP klientské počítače s nejsnadnější správou v podnikovém prostředí.

Aktualizace a správa softwaru

Společnost HP poskytuje několik nástrojů pro správu a aktualizaci softwaru ve stolních počítačích a pracovních stanicích. Jsou to nástroje Altiris, Altiris PC Transplant Pro, HP Client Manager Software (řešení společnosti Altiris), System Software Manager, Proactive Change Notification a ActiveUpdate.

Nástroj HP Client Manager Software

Inteligentní nástroj HP Client Manager Software (HP CMS) úzce integruje technologii HP Intelligent Manageability v rámci nástroje Altiris a poskytuje tak vynikající funkce pro správu hardwaru zařízení společnosti HP pro přístup. Patří k nim následující funkce:

- podrobné zobrazení inventáře hardwaru pro správu prostředků,
- sledování a diagnostika stavu osobního počítače,
- aktivní upozorňování na změny hardwaru,
- podávání zpráv (prostřednictvím webu) o důležitých událostech, jako jsou například varování týkající se teploty počítače nebo výstrahy týkající se paměti,
- vzdálená aktualizace systémového softwaru, například ovladačů zařízení a systému ROM BIOS,
- vzdálená změna pořadí spouštění.

Další informace o nástroji HP Client Manager naleznete na adrese http://h18000.www1.hp.com/im/client_mgr.html.

Řešení společnosti Altiris

Řešení HP Client Management Solutions nabízejí centralizovanou správu hardwaru klientských zařízení HP pro všechny oblasti životního cyklu IT.

- Správa inventáře a prostředků
  - Vyhovění licenci na software
  - Sledování počítače a hlášení
  - Leasingová smlouva, opravy sledování majetku
- Zavedení a přenesení
  - Přenesení v systémech Microsoft Windows 2000 nebo Windows XP Professional nebo Home Edition
  - Zavedení systému
  - Přenesení personality (osobní nastavení a úpravy)
- Technická podpora a řešení problémů
  - Správa lístků technické podpory
  - Vzdálené odstraňování potíží
  - Vzdálené řešení problémů
  - Obnovení klienta po havárii
- Správa softwaru a operací
  - Neustálá správa plochy
  - Zavedení softwaru systému HP
  - Automatické opravy aplikací

U vybraných modelů stolních počítačů a notebooků je agent pro správu Altiris dodáván jako součást továrně instalované bitové kopie (snímku). Tento agent umožňuje komunikovat s řešením Altiris Development Solution, které lze použít k zavedení nového hardwaru nebo přenesení personality do nového operačního systému pomocí průvodců se snadným ovládáním. Řešení Altiris poskytují funkce pro snadnou distribuci softwaru. Pokud jsou použita spolu s nástrojem System Software Manager nebo HP Client Manager, mohou správci také aktualizovat systém ROM BIOS a ovladače zařízení z centrální konzoly.

Další informace najdete na webu http://www.hp.com/go/easydeploy.

Nástroj Altiris PC Transplant Pro

Nástroj Altiris PC Transplant Pro umožňuje bezproblémové přenesení osobních počítačů do nového prostředí tak, že zachová původní nastavení, předvolby a data. Přenos je rychlý a snadný. Inovace již nebudou trvat hodiny či dny, ale pouze minuty, a stolní počítač bude vypadat a fungovat přesně tak, jak uživatelé očekávají.

Další informace a podrobnosti týkající se stažení plně funkční 30denní zkušební verze naleznete na adrese http://h18000.www1.hp.com/im/prodinfo.html#deploy.

Nástroj System Software Manager

Nástroj System Software Manager (SSM) umožňuje aktualizovat systémový software ve více počítačích současně. Po spuštění v systému klientského počítače nástroj SSM zjistí verze softwaru i hardwaru a poté aktualizuje příslušný software z hlavního úložiště, nazývaného také úložiště souborů. Verze ovladačů podporované nástrojem SSM jsou na webovém serveru umožňujícím stažení ovladačů a na disku CD-ROM Support Software (Podpůrný software) označeny zvláštní ikonou. Další informace o nástroji SSM a možnost jeho stažení naleznete na adrese http://h18000.www1.hp.com/im/ssmwp.html.

Program Proactive Change Notification

Program Proactive Change Notification používá webový server Subscriber's Choice a umožňuje aktivní a automatické provádění následujících úloh:

- Odesílání e-mailových zpráv PCN (Proactive Change Notification), které upozorňují na změny hardwaru a softwaru u většiny komerčních počítačů a serverů, a to až 60 dní předem.
- Odesílání e-mailových zpráv obsahujících zprávy typu Customer Bulletins, Customer Advisories, Customer Notes, Security Bulletins a Driver Alerts pro většinu komerčních počítačů a serverů.

Můžete vytvořit vlastní profil a zajistit tak, že budete dostávat pouze informace vztahující se ke specifickému prostředí informačních technologií (IT). Další informace o programu Proactive Change Notification a možnost vytvoření upraveného profilu najdete na webu http://www.hp.com/go/pcn.

Aplikace ActiveUpdate

Aplikace ActiveUpdate je klientská aplikace společnosti HP. Klient ActiveUpdate je spuštěn v místním systému a pomocí profilu definovaného uživatelem aktivně a automaticky stahuje aktualizace softwaru pro většinu komerčních počítačů a serverů společnosti HP. Tyto stažené softwarové aktualizace lze inteligentně zavést do počítačů, pro které jsou určeny, pomocí programů HP Client Manager Software a System Software Manager.

Chcete-li zjistit další informace o programu ActiveUpdate, stáhnout jej a vytvořit si vlastní profil, přejděte na adresu http://h18000.www1.hp.com/products/servers/management/activeupdate/index.html.

Paměť ROM typu flash

Počítač je dodáván s programovatelnou pamětí ROM (Read Only Memory) typu flash. Vytvoříte-li pomocí nástroje Computer Setup (F10) heslo pro nastavení, můžete paměť ROM chránit před nechtěnou aktualizací nebo neúmyslným přepsáním. To je důležité k zajištění provozní integrity počítače. Jestliže chcete nebo potřebujete inovovat paměť ROM, můžete postupovat následujícím způsobem:

- Objednejte si u společnosti HP disketu s inovací ROMPaq.
- Stáhněte si nejnovější bitové kopie inovace ROMPaq na adrese http://h18000.www1.hp.com/im/ssmwp.html.

UPOZORNÌNÍ: Chcete-li zajistit maximální ochranu paměti ROM, vytvořte heslo pro nastavení. Toto heslo brání neoprávněným inovacím paměti ROM. Nástroj System Software Manager umožňuje správci systému nastavit heslo pro nastavení u několika počítačů současně. Další informace naleznete na adrese http://h18000.www1.hp.com/im/ssmwp.html.

Vzdálená paměť ROM typu flash

Vzdálená aktualizace paměti ROM typu flash umožňuje správci systému bezpečně aktualizovat paměť ROM ve vzdálených počítačích HP přímo z centrální konzoly pro správu sítě. Provedení tohoto úkolu vzdáleně ve více počítačích zajistí jednotné zavedení a větší kontrolu nad bitovými kopiemi paměti ROM v počítačích HP v síti. Zlepší se také produktivita a sníží celkové náklady na vlastnictví.

Chcete-li použít vzdálenou paměť ROM typu flash, musí být počítač zapnut nebo aktivován pomocí funkce Remote Wakeup (Vzdálené spuštění).

Další informace o vzdálené paměti ROM typu flash naleznete v části věnované nástroji HP Client Manager Software nebo System Software Manager na serveru http://h18000.www1.hp.com/im/prodinfo.html.

HPQFlash

Nástroj HPQFlash slouží k místní aktualizaci nebo obnovení systémové paměti ROM v jednotlivých počítačích prostřednictvím systému Windows.

Další informace o nástroji HPQFlash najdete na webu http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18607.html.

Paměť ROM s blokem pro bezpečné zavedení (FailSafe Boot Block ROM)

Paměť ROM s blokem pro bezpečné zavedení (FailSafe Boot Block ROM) umožňuje obnovení systému při velmi nepravděpodobném případě selhání paměti ROM typu flash, například při výpadku napájení v průběhu aktualizace paměti ROM. Zaváděcí blok je část paměti ROM chráněná před aktualizací typu flash, která při každém zapnutí počítače kontroluje a ověřuje funkčnost systémové paměti ROM typu flash.

- Pokud je systémová paměť ROM platná, systém se normálně spustí.
- Jestliže kontrola ověření systémové paměti ROM selže, zabezpečí paměť ROM s blokem pro bezpečné zavedení (FailSafe Boot Block ROM) dostatečnou podporu ke spuštění systému z diskety ROMPaq, která systémové paměti ROM poskytne platnou bitovou kopii softwaru.

V případě, že zaváděcí blok zjistí neplatnou systémovou paměť ROM, kontrolka napájení osmkrát ČERVENĚ zabliká vždy po 1 sekundě s dvousekundovou pauzou. Zároveň osmkrát zazní zvukový signál. Na obrazovce se zobrazí zpráva režimu obnovení zaváděcím blokem paměti ROM (u některých modelů).

Systém, který přešel do režimu obnovení zaváděcím blokem paměti ROM, obnovíte provedením následujících kroků:

1. Pokud je v disketové jednotce disketa, vyjměte ji a vypněte napájení.
2. Do disketové jednotky vložte disketu ROMPaq.
3. Zapněte počítač.
4. Jestliže nebyla žádná disketa ROMPaq nalezena, zobrazí se výzva k jejímu vložení a restartování počítače.
5. Pokud bylo vytvořeno heslo pro nastavení, rozsvítí se indikátor klávesy Caps Lock a zobrazí se výzva k zadání hesla.
6. Zadejte heslo pro nastavení.
7. Dojde-li k úspěšnému spuštění systému z diskety a přeprogramování paměti ROM, rozsvítí se tři indikátory na klávesnici. Úspěšné ukončení bude signalizováno také sledem zvyšujících se zvukových signálů.
8. Vyjměte disketu a vypněte počítač.
9. Znovu zapněte počítač. Dojde k jeho restartování.

V následující tabulce jsou uvedeny různé kombinace indikátorů na klávesnici používané zaváděcím blokem paměti ROM (je-li k počítači připojena klávesnice PS/2), význam jednotlivých kombinací a stav či požadovaná činnost.

Kombinace indikátorů na klávesnici používané zaváděcím blokem paměti ROM

Režim bloku pro bezpečné zavedení	Barva indikátoru na klávesnici	Činnost indikátoru na klávesnici	Stav nebo význam
Num Lock	Zelená	Svítí	Disketa ROMPaq nebyla nalezena, je chybná nebo jednotka není připravena.
Caps Lock	Zelená	Svítí	Zadejte heslo.
Num, Caps, Scroll Lock	Zelená	Blikají jeden po druhém, Num Lock, Caps Lock, Scroll Lock.	Klávesnice je zamknuta v síťovém režimu.
Num, Caps, Scroll Lock	Zelená	Svítí	Aktualizace zaváděcího bloku paměti ROM proběhla úspěšně. Vypněte počítač a znovu jej zapněte.

✎ U klávesnic USB diagnostické indikátory neblikají.

Replikace nastavení

Následující postupy umožňují správci snadno kopírovat konfiguraci nastavení mezi počítači stejného modelu. Lze tak rychleji a konzistentněji nakonfigurovat více počítačů.

Oba postupy vyžadují disketovou jednotku nebo podporované zařízení USB typu flash, například modul HP Drive Key.

Kopírování do jednoho počítače

UPOZORNĚNÍ: Konfigurace nastavení závisí na modelu. Pokud zdrojový a cílový počítač nejsou shodné modely, může dojít k poškození systému souborů. Nekopírujte například konfiguraci nastavení ze stolního počítače D510 Ultra-slim Desktop do počítače D510 e-pc.

1. Vyberte konfiguraci nastavení, kterou chcete kopírovat. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnosti **Start > Vypnout > Restartovat počítač**.
2. Jakmile se indikátor monitoru rozsvítí zeleně, stiskněte klávesu **F10**. V případě potřeby můžete stisknutím klávesy **ENTER** přeskočit úvodní obrazovku.

Jestliže klávesu **F10** nestisknete ve vhodné době, bude nutné počítač vypnout, znovu zapnout a znovu stisknout klávesu **F10**.

3. Vložte disketu nebo zařízení pro média USB typu flash.
4. Klepněte na možnost **File** (Soubor) > **Save to Diskette** (Uložit na disketu). Podle pokynů na obrazovce vytvořte konfigurační disketu nebo zařízení USB typu flash.
5. Vypněte konfigurovaný počítač a vložte konfigurační disketu nebo zařízení USB typu flash.
6. Zapněte konfigurovaný počítač. Jakmile se indikátor monitoru rozsvítí zeleně, stiskněte klávesu **F10**. V případě potřeby můžete stisknutím klávesy **ENTER** přeskočit úvodní obrazovku.
7. Klepněte v nabídce **File** (Soubor) na příkaz **Restore from Diskette** (Obnovit z diskety) a postupujte podle pokynů na obrazovce.
8. Po dokončení konfigurace restartujte počítač.

Kopírování do více počítačů

UPOZORNĚNÍ: Konfigurace nastavení závisí na modelu. Pokud zdrojový a cílový počítač nejsou shodné modely, může dojít k poškození systému souborů. Nekopírujte například konfiguraci nastavení ze stolního počítače D510 Ultra-slim Desktop do počítače D510 e-pc.

U tohoto způsobu trvá o něco déle příprava konfigurační diskety nebo zařízení USB typu flash, ale kopírování konfigurace do cílových počítačů je značně rychlejší.

Spouštěcí disketu nelze vytvořit v systému Windows 2000. K tomuto postupu je nutná spouštěcí disketa nebo spouštěcí zařízení USB typu flash. Pokud nemáte k dispozici systémy Windows 9x nebo Windows XP, ve kterých by bylo možné vytvořit spustitelnou disketu, použijte metodu kopírování do jednoho počítače (viz část „Kopírování do jednoho počítače na stránce 11“).

1. Vytvořte spouštěcí disketu nebo zařízení pro média USB typu flash. Viz část „Spouštěcí disketa na stránce 13“, „Podporované zařízení USB typu flash na stránce 13“ nebo „Nepodporované zařízení USB typu flash na stránce 17“.

UPOZORNĚNÍ: Ze zařízení USB typu flash nelze spouštět všechny počítače. Pokud je ve výchozím pořadí spouštění v seznamu nástroje Computer Setup (F10) uvedeno zařízení USB před pevným diskem, lze počítač spustit ze zařízení USB typu flash. Jinak je nutné použít spouštěcí disketu.

2. Vyberte konfiguraci nastavení, kterou chcete kopírovat. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnosti **Start > Vypnout > Restartovat počítač**.
3. Jakmile se indikátor monitoru rozsvítí zeleně, stiskněte klávesu **F10**. V případě potřeby můžete stisknutím klávesy **ENTER** přeskočit úvodní obrazovku.

Jestliže klávesu **F10** nestisknete ve vhodné době, bude nutné počítač vypnout, znovu zapnout a znovu stisknout klávesu **F10**.

4. Vložte spouštěcí disketu nebo zařízení pro média USB typu flash.

5. Zvolte tyto možnosti: **File (Soubor) > Save to Diskette (Uložit na disketu)**. Podle pokynů na obrazovce vytvořte konfigurační disketu nebo zařízení USB typu flash.
6. Stáhněte nástroj BIOS pro replikaci nastavení (repset.exe) a zkopírujte jej na konfigurační disketu nebo zařízení USB typu flash. Nástroj najdete na webu http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18040.html.
7. Vytvořte na konfigurační disketě nebo zařízení USB typu flash soubor autoexec.bat s následujícím příkazem:

   repset.exe

8. Vypněte konfigurovaný počítač. Vložte konfigurační disketu nebo zařízení USB typu flash a zapněte počítač. Konfigurační nástroj bude automaticky spuštěn.
9. Po dokončení konfigurace restartujte počítač.

Vytvoření spouštěcího zařízení

Spouštěcí disketa

Tyto pokyny platí pro systémy Windows XP Professional a Home Edition. Systém Windows 2000 nepodporuje vytváření spouštěcích disket.

1. Do disketové jednotky vložte disketu.
2. Klepněte na tlačítko **Start** a potom na příkaz **Tento počítač**.
3. Pravým tlačítkem myši klepněte na jednotku diskety a klepněte na příkaz **Naformátovat**.
4. Zaškrtněte políčko **Vytvořit spouštěcí disketu MS-DOS** a klepněte na tlačítko **Spustit**.

Vraťte se na část „Kopírování do více počítačů na stránce 12“.

Podporované zařízení USB typu flash

Podporovaná zařízení, například HP Drive Key nebo DiskOnKey, obsahují předinstalovanou bitovou kopii, která zjednodušuje proces jejich změny na spouštěcí zařízení. Pokud používané zařízení Drive Key tuto bitovou kopii neobsahuje, pokračujte postupem dále v této části (viz část „Nepodporované zařízení USB typu flash na stránce 17“).

UPOZORNĚNÍ: Ze zařízení USB typu flash nelze spouštět všechny počítače. Pokud je ve výchozím pořadí spouštění v seznamu nástroje Computer Setup (F10) uvedeno zařízení USB před pevným diskem, lze počítač spustit ze zařízení USB typu flash. Jinak je nutné použít spouštěcí disketu.

K vytvoření spouštěcího zařízení USB typu flash potřebujete:

- Jeden z následujících systémů:
  - stolní počítač Compaq Evo D510 Ultra-slim,
  - počítač Compaq Evo D510 v provedení Convertible Minitower/Small Form Factor,
  - stolní počítač HP Compaq d530 Series – provedení Ultra-slim Desktop, Small Form Factor nebo Convertible Minitower,
  - notebook Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c nebo N1000c,
  - notebook Compaq Presario 1500 nebo 2800.

  V závislosti na jednotlivých systémech BIOS mohou budoucí systémy také podporovat spouštění ze zařízení HP Drive Key.

UPOZORNĚNÍ: Pokud používáte jiný počítač než výše uvedené, musí se ve výchozím pořadí spouštění v nástroji Computer Setup (F10) nacházet zařízení USB před pevným diskem.

- Jeden z následujících modulů pro ukládání dat:
  - 16MB HP Drive Key,
  - 32MB HP Drive Key,
  - 32MB DiskOnKey,
  - 64MB HP Drive Key,
  - 64MB DiskOnKey,
  - 128MB HP Drive Key,
  - 128MB DiskOnKey.

- Spouštěcí disketu pro systém DOS s programy FDISK a SYS. Není-li program SYS k dispozici, lze použít program FORMAT, ale dojde ke ztrátě všech souborů v modulu Drive Key.

1. Vypněte počítač.
2. Vložte modul Drive Key do jednoho z portů USB v počítači a vyjměte všechna ostatní zařízení USB pro ukládání dat kromě disketových jednotek USB.
3. Vložte spouštěcí disketu DOS s programem FDISK.COM a programem SYS.COM nebo FORMAT.COM do disketové jednotky a zapněte počítač, který se spustí z diskety DOS.
4. Spusťte program FDISK z příkazového řádku A:\ zadáním příkazu **FDISK** a stisknutím klávesy ENTER. Pokud se zobrazí výzva k povolení podpory velkých disků, klepněte na možnost **Yes** (**Y**).
5. Zadáním volby Choice [**5**] zobrazte jednotky v systému. Modul Drive Key bude jednotkou, která se blíží velikosti jedné z uvedených jednotek. Obvykle půjde o poslední jednotku v seznamu. Poznamenejte si písmeno jednotky.

   Jednotka Drive Key: _____

UPOZORNĚNÍ: Pokud se žádná jednotka neshoduje s modulem Drive Key, nepokračujte. Může dojít ke ztrátě dat. Zkontrolujte všechny porty USB, zda neobsahují další zařízení pro ukládání dat. Pokud nějaká najdete, odeberte je, restartujte počítač a pokračujte od kroku 4. Jestliže žádná nenajdete, systém nepodporuje moduly Drive Key nebo je modul Drive Key vadný. NEPOKOUŠEJTE SE dále převést modul Drive Key na spouštěcí.

6. Ukončete program FDISK stisknutím klávesy **ESC**, která vás vrátí na příkazový řádek A:\.
7. Pokud spouštěcí disketa DOS obsahuje program SYS.COM, přejděte ke kroku 8. Jinak pokračujte krokem 9.
8. Na příkazovém řádku A:\ zadejte **SYS x:** kde x představuje písmeno jednotky poznamenané výše. Přejděte ke kroku 13.

UPOZORNĚNÍ: Je nutné, abyste zadali správné písmeno jednotky modulu Drive Key.

Po přenosu systémových souborů se program SYS vrátí na příkazový řádek A:\.

9. Zkopírujte všechny soubory, které si chcete uchovat, z modulu Drive Key do dočasné složky na jiné jednotce (například interní pevný disk systému).
10. Na příkazovém řádku A:\ zadejte **FORMAT /S X:** kde X představuje písmeno jednotky poznamenané dříve.

UPOZORNĚNÍ: Je nutné, abyste zadali správné písmeno jednotky modulu Drive Key.

Program FORMAT zobrazí jedno nebo více upozornění a pokaždé se zeptá, zda chcete pokračovat. Zadejte vždy **y**. Program FORMAT zformátuje modul Drive Key, přidá systémové soubory a požádá o jmenovku svazku (Volume Label).

11. Pokud žádnou jmenovku zadávat nechcete, stiskněte klávesu **ENTER**. Jinak zadejte požadovanou jmenovku.
12. Zkopírujte všechny soubory uložené v kroku 9 zpět do modulu Drive Key.
13. Vyjměte disketu a restartujte počítač. Počítač bude spuštěn z modulu Drive Key jako jednotka C.

Výchozí pořadí spouštění se mezi počítači liší a lze je změnit v nástroji Computer Setup (F10).

Pokud jste použili verzi DOS ze systému Windows 9x, zobrazí se pravděpodobně nakrátko obrazovka s logem Windows. Pokud tuto obrazovku nechcete, přidejte soubor s nulovou délkou nazvaný LOGO.SYS do kořenového adresáře modulu Drive Key.

Vraťte se na část „Kopírování do více počítačů na stránce 12“.

Nepodporované zařízení USB typu flash

UPOZORNĚNÍ: Ze zařízení USB typu flash nelze spouštět všechny počítače. Pokud je ve výchozím pořadí spouštění v seznamu nástroje Computer Setup (F10) uvedeno zařízení USB před pevným diskem, lze počítač spustit ze zařízení USB typu flash. Jinak je nutné použít spouštěcí disketu.

K vytvoření spouštěcího zařízení USB typu flash potřebujete:

- Jeden z následujících systémů:
  - stolní počítač Compaq Evo D510 Ultra-slim,
  - počítač Compaq Evo D510 v provedení Convertible Minitower/Small Form Factor,
  - stolní počítač HP Compaq d530 Series – provedení Ultra-slim Desktop, Small Form Factor nebo Convertible Minitower,
  - notebook Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c nebo N1000c,
  - notebook Compaq Presario 1500 nebo 2800.

  V závislosti na jednotlivých systémech BIOS mohou budoucí systémy také podporovat spouštění ze zařízení USB typu flash.

UPOZORNĚNÍ: Pokud používáte jiný počítač než výše uvedené, musí se ve výchozím pořadí spouštění v nástroji Computer Setup (F10) nacházet zařízení USB před pevným diskem.

- Spouštěcí disketu pro systém DOS s programy FDISK a SYS. Není-li program SYS k dispozici, lze použít program FORMAT, ale dojde ke ztrátě všech souborů v modulu Drive Key.

1. Pokud systém obsahuje karty PCI s připojenými jednotkami SCSI, ATA RAID nebo SATA, vypněte počítač a odpojte síťovou šňůru.

UPOZORNĚNÍ: Síťová šňůra MUSÍ být vytažena ze zásuvky.

2. Otevřete počítač a vyjměte karty PCI.
3. Vložte zařízení USB typu flash do jednoho z portů USB v počítači a vyjměte všechna ostatní zařízení USB pro ukládání dat kromě disketových jednotek USB. Zavřete kryt počítače.
4. Připojte síťovou šňůru a zapněte počítač. Jakmile se indikátor monitoru rozsvítí zeleně, přejděte stisknutím klávesy **F10** do nástroje Computer Setup.

5. Přejděte do nabídky Advanced/PCI devices (Pokročilé/zařízení PCI) a zakažte řadiče IDE i SATA. Při zakazování řadiče SATA si poznamenejte hodnotu IRQ, ke které je řadič přiřazen. Tuto hodnotu bude nutné později znovu přiřadit. Ukončete program Setup a potvrďte změny.

   Hodnota IRQ pro řadič SATA: _____

6. Vložte spouštěcí disketu DOS s programem FDISK.COM a programem SYS.COM nebo FORMAT.COM do disketové jednotky a zapněte počítač, který se spustí z diskety DOS.
7. Spusťte program FDISK a odstraňte všechny existující oddíly na zařízení USB typu flash. Vytvořte nový oddíl a označte jej jako aktivní. Stisknutím klávesy **ESC** ukončete program FDISK.
8. Pokud se po ukončení programu FDISK systém automaticky nerestartuje, stiskněte klávesy **CTRL**+**ALT**+**DEL** a restartujte jej z diskety DOS.
9. Na příkazovém řádku A:\ zadejte **FORMAT C: /S** a stiskněte klávesu **ENTER**. Program FORMAT zformátuje zařízení USB typu flash, přidá systémové soubory a požádá o jmenovku svazku (Volume Label).
10. Pokud žádnou jmenovku zadávat nechcete, stiskněte klávesu **ENTER**. Jinak zadejte požadovanou jmenovku.
11. Vypněte počítač a odpojte síťovou šňůru. Otevřete počítač a nainstalujte znovu dříve vyjmuté karty PCI. Zavřete kryt počítače.
12. Připojte síťovou šňůru, vyjměte disketu a zapněte počítač.
13. Jakmile se indikátor monitoru rozsvítí zeleně, přejděte stisknutím klávesy **F10** do nástroje Computer Setup.
14. Přejděte do nabídky Advanced/PCI Devices a znovu povolte řadiče IDE a SATA, které jste zakázali v kroku 5. Nastavte u řadiče SATA původní hodnotu IRQ.
15. Uložte změny a ukončete program. Počítač bude spuštěn ze zařízení USB typu flash jako jednotka C.

✎ Výchozí pořadí spouštění se mezi počítači liší a lze je změnit v nástroji Computer Setup (F10).

Pokud jste použili verzi DOS ze systému Windows 9x, zobrazí se pravděpodobně nakrátko obrazovka s logem Windows. Pokud tuto obrazovku nechcete, přidejte soubor s nulovou délkou nazvaný LOGO.SYS do kořenového adresáře modulu Drive Key.

Vraťte se na část „Kopírování do více počítačů na stránce 12“.

Dvoupolohový přepínač režimů napájení

Pokud je v systému Windows 2000 a Windows XP Professional nebo Home Edition povoleno rozhraní ACPI (Advanced Configuration and Power Interface), může vypínač napájení počítač zapnout, vypnout nebo převést do režimu spánku. V režimu spánku není počítač zcela vypnut, ale je převeden do režimu nízké spotřeby energie. Tento postup umožňuje rychlé vypnutí počítače bez nutnosti zavřít aplikace a také rychlý návrat ke stejnému provoznímu stavu bez ztráty dat.

Chcete-li změnit konfiguraci vypínače napájení, proveďte následující kroky:

1. V systému Windows 2000 klepněte levým tlačítkem myši na tlačítko **Start** a pak zvolte možnosti **Nastavení > Ovládací panely > Možnosti napájení**.

   V systému Windows XP Professional a Home Edition klepněte levým tlačítkem myši na tlačítko **Start** a pak zvolte možnosti **Ovládací panely > Výkon a údržba > Možnosti napájení**.

2. V okně **Možnosti napájení – vlastnosti** klepněte na kartu **Upřesnit**.
3. V části **Tlačítka napájení** vyberte požadované nastavení vypínače napájení.

Pokud vypínač napájení nakonfigurujete tak, aby sloužil pro přechod do režimu spánku, způsobí stisknutí vypínače přechod systému do režimu nízké spotřeby energie (režim spánku). Opětovným stisknutím vypínače rychle převedete systém do plného provozního stavu. Chcete-li systém zcela vypnout, stiskněte vypínač a podržte jej po dobu čtyř sekund.

UPOZORNĚNÍ: Nepoužívejte vypínač k vypnutí počítače s výjimkou případu, že systém nereaguje. Vypnutí počítače bez interakce s operačním systémem může způsobit poškození nebo ztrátu dat na pevném disku.

Server WWW

Technici společnosti HP pečlivě testují a ladí software společnosti HP i software jiných výrobců a vyvíjejí podpůrný software pro konkrétní operační systémy, aby zajistili nejvyšší úroveň výkonu, kompatibility a spolehlivosti počítačů HP.

Při přechodu na nový nebo vylepšený operační systém je velmi důležitá implementace podpůrného softwaru určeného pro příslušný operační systém. Jestliže plánujete použití verze systému Microsoft Windows, která se liší od verze dodávané s počítačem, je nutné nainstalovat odpovídající nástroje a ovladače zařízení, aby byla zajištěna podpora a správné fungování všech funkcí.

Společnost HP již vyřešila problém umístění, přístupu, hodnocení a instalace nejnovějších verzí podpůrného softwaru. Software lze stáhnout ze serveru http://www.hp.com/support.

Na tomto webovém serveru jsou k dispozici nejnovější ovladače zařízení, nástroje a bitové kopie paměti ROM typu flash potřebné ke spuštění nejnovějšího operačního systému Microsoft Windows v počítači HP.

Stavební bloky a partneři

Produkty pro správu společnosti HP jsou integrovány s dalšími aplikacemi pro správu systému a jsou založeny na následujících standardech:

- standard DMI 2.0 (Desktop Management Interface),
- technologie Wake on LAN,
- rozhraní ACPI,
- systém SM BIOS (System Management BIOS),
- podpora prostředí PXE (Pre-boot Execution).

Evidence inventárních čísel a zabezpečení

Funkce evidence inventárních čísel obsažené v počítači poskytují důležité údaje evidence inventárních čísel, které lze spravovat pomocí produktů HP Insight Manager a dalších aplikací pro správu systému. Bezproblémová automatická integrace mezi funkcí evidence inventárních čísel a těmito produkty umožňuje zvolit nástroj pro správu, který nejlépe odpovídá vašemu prostředí, a maximálně zhodnotit investice do stávajících nástrojů.

Společnost HP také nabízí několik produktů pro řízení přístupu k cenným součástem a informacím. Funkce Embedded Security nástroje ProtectTools (je-li nainstalovaná), zabraňuje neoprávněnému přístupu k datům, kontroluje integritu systému a ověřuje uživatele třetí strany, kteří se pokoušejí vstoupit do systému. Funkce zabezpečení, například ProtectTools, senzor zámku počítačové skříně (Smart Cover Sensor) a zámek počítačové skříně (Smart Cover Lock), které jsou dostupné u vybraných modelů, pomáhají zabránit neoprávněnému přístupu k vnitřním součástem počítače. Zákazem paralelních nebo sériových portů či portů USB nebo zákazem možnosti spuštění z vyměnitelných médií můžete chránit cenné inventarizační informace. Upozornění na změnu paměti (Memory Change) a upozornění senzoru zámku počítačové skříně (Smart Cover Sensor) mohou být automaticky směrována aplikacím pro správu systému, což zajistí aktivní upozornění na manipulaci s vnitřními součástmi počítače.

U některých systémů jsou volitelně k dispozici nástroje Protect Tools, senzor zámku počítačové skříně (Smart Cover Sensor) a zámek počítačové skříně (Smart Cover Lock).

Nastavení zabezpečení v počítačích společnosti HP provádějte pomocí následujících nástrojů:

- Místně, pomocí nástroje Computer Setup. Další informace a pokyny týkající se použití nástroje Computer Setup naleznete v *Příručce k nástroji Computer Setup (F10)* dodané s počítačem.
- Vzdáleně, pomocí nástroje HP Client Manager nebo System Software Manager. Tento software umožňuje spolehlivé a jednotné zavedení a řízení nastavení zabezpečení prostřednictvím jednoduchého nástroje příkazového řádku.

Následující tabulka a části obsahují informace týkající se místní správy funkcí zabezpečení počítače pomocí nástroje Computer Setup (F10).

Přehled funkcí zabezpečení

Funkce	Účel	Způsob nastavení
Řízení možnosti spouštění z vyměnitelných médií	Zabraňuje spuštění systému z médií ve vyměnitelných jednotkách. (k dispozici u některých jednotek)	Z nabídky nástroje Computer Setup (F10)
Řízení sériového, paralelního nebo infračerveného rozhraní nebo rozhraní USB	Zabraňuje přenosu dat prostřednictvím integrovaného sériového, paralelního nebo infračerveného rozhraní nebo rozhraní USB (Universal Serial Bus).	Z nabídky nástroje Computer Setup (F10)
Power-On Password (Heslo pro spuštění)	Zabraňuje použití počítače, pokud není zadáno heslo. Může se týkat počátečního spuštění systému i restartování.	Z nabídky nástroje Computer Setup (F10)
Setup Password (Heslo pro nastavení)	Zabraňuje změně konfigurace počítače (použití nástroje Computer Setup), pokud není zadáno heslo.	Z nabídky nástroje Computer Setup (F10)
Zařízení Embedded Security (Integrované zabezpečení)	Pomocí šifrování a ochrany heslem zabraňuje neoprávněnému přístupu k datům. Kontroluje integritu systému a ověřuje uživatele třetí strany, kteří se pokoušejí vstoupit do systému.	Z nabídky nástroje Computer Setup (F10)
DriveLock	Zabraňuje neoprávněnému přístupu k datům na pevných discích v multifunkční pozici. Tato funkce je k dispozici pouze u vybraných modelů.	Z nabídky nástroje Computer Setup (F10)

✎ Další informace o nástroji Computer Setup naleznete v *Příručce k nástroji Computer Setup (F10)*. Podpora funkcí zabezpečení se může lišit v závislosti na konkrétní konfiguraci počítače.

Přehled funkcí zabezpečení *(pokračování)*

Funkce	Účel	Způsob nastavení
Senzor zámku počítačové skříně (Smart Cover Sensor)	Informuje, že došlo k sejmutí krytu nebo bočního panelu počítače. Lze nastavit tak, aby po sejmutí krytu nebo bočního panelu počítače bylo k restartování počítače vyžadováno heslo pro nastavení. Další informace o této funkci naleznete v *Referenční příručce k hardwaru* na disku CD-ROM *Knihovna dokumentace*. Tato funkce je k dispozici pouze u vybraných modelů.	Z nabídky nástroje Computer Setup (F10)
Master Boot Record Security (Hlavní spouštěcí záznam)	Může předejít neúmyslným změnám nebo záměrnému poškození hlavního spouštěcího záznamu na aktuálním spouštěcím disku a poskytuje prostředky k obnovení posledního známého platného hlavního spouštěcího záznamu.	Z nabídky nástroje Computer Setup (F10)
Upozornění na změnu paměti	Zjistí přidání, přesun či odstranění paměťových modulů a upozorní uživatele a správce systému.	Informace o aktivaci funkce upozornění na změnu paměti získáte v příručce online *Intelligent Manageability Guide*.

✎ Další informace o nástroji Computer Setup naleznete v *Příručce k nástroji Computer Setup (F10)*. Podpora funkcí zabezpečení se může lišit v závislosti na konkrétní konfiguraci počítače.

Přehled funkcí zabezpečení *(pokračování)*

Funkce	Účel	Způsob nastavení
Označení vlastnictví	Během spuštění systému (chráněného heslem pro nastavení) zobrazí informace o vlastnictví zadané správcem systému.	Z nabídky nástroje Computer Setup (F10)
Zajištění pro lankový zámek	Omezuje přístup k vnitřním částem počítače a zabraňuje tak nechtěným změnám konfigurace nebo vyjímání součástí. Může být využit také k upevnění počítače k pevnému předmětu a zajištění proti krádeži.	Chcete-li počítač upevnit k pevnému objektu, nainstalujte lankový zámek.
Bezpečnostní smyčka	Omezuje přístup k vnitřním částem počítače a zabraňuje tak nechtěným změnám konfigurace nebo vyjímání součástí.	Chcete-li zabránit nechtěným změnám konfigurace nebo vyjímání součástí, nainstalujte do bezpečností smyčky zámek.

✎ Další informace o nástroji Computer Setup naleznete v *Příručce k nástroji Computer Setup (F10)*. Podpora funkcí zabezpečení se může lišit v závislosti na konkrétní konfiguraci počítače.

Zabezpečení pomocí hesla

Heslo pro spuštění zabraňuje neoprávněnému použití počítače, neboť při každém spuštění nebo restartování počítače je vyžadováno zadání hesla pro přístup k aplikacím či datům. Heslo pro nastavení zabraňuje neoprávněnému přístupu k nástroji Computer Setup. Lze jej také použít jako nadřazené heslo namísto hesla pro spuštění. To znamená, že pokud po výzvě k zadání hesla pro spuštění zadáte heslo pro nastavení, budete moci počítač používat.

Je možné vytvořit heslo pro nastavení platné pro celou síť, které správci systému umožní přihlášení ke všem počítačům v síti a jejich správu, aniž by znal případné heslo pro spuštění.

Vytvoření hesla pro nastavení pomocí nástroje Computer Setup

Je-li systém vybaven zařízením Embedded Security, projděte si část „Embedded Security (Integrované zabezpečení) na stránce 30“.

Vytvoření hesla pro nastavení pomocí nástroje Computer Setup zabrání změně konfigurace počítače (použití nástroje Computer Setup(F10)), pokud není zadáno heslo.

1. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnosti **Start > Vypnout > Restartovat počítač**.
2. Jakmile se indikátor monitoru rozsvítí zeleně, stiskněte klávesu **F10**. V případě potřeby můžete stisknutím klávesy **ENTER** přeskočit úvodní obrazovku.

Jestliže klávesu **F10** nestisknete ve vhodné době, bude nutné počítač vypnout, znovu zapnout a znovu stisknout klávesu **F10**.

3. V nabídce **Security** (Zabezpečení) vyberte příkaz **Setup Password** (Heslo pro nastavení) a postupujte podle pokynů na obrazovce.
4. Před ukončením práce zvolte možnost **File (Soubor) > Save Changes and Exit (Uložit změny a ukončit program)**.

Zadání hesla pro spuštění pomocí nástroje Computer Setup

Vytvoření hesla pro spuštění pomocí nástroje Computer Setup zabraňuje použití počítače po jeho spuštění, pokud není zadáno heslo. Pokud je heslo pro spuštění nastaveno, zobrazí nástroj Computer Setup v nabídce Security (Zabezpečení) možnosti Password Options (Možnosti nastavení hesla). Jednou z těchto možností je Password Prompt on Warm Boot (Požadovat heslo při restartování). Jestliže je možnost Password Prompt on Warm Boot povolena, musí být heslo zadáno také při každém restartování počítače.

1. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnosti **Start > Vypnout > Restartovat počítač**.
2. Jakmile se indikátor monitoru rozsvítí zeleně, stiskněte klávesu **F10**. V případě potřeby můžete stisknutím klávesy **ENTER** přeskočit úvodní obrazovku.

Jestliže klávesu **F10** nestisknete ve vhodné době, bude nutné počítač vypnout, znovu zapnout a znovu stisknout klávesu **F10**.

3. V nabídce **Security** (Zabezpečení) vyberte příkaz **Power-On Password** (Heslo pro spuštění) a postupujte podle pokynů na obrazovce.
4. Před ukončením práce zvolte možnost **File (Soubor) > Save Changes and Exit (Uložit změny a ukončit program)**.

Zadání hesla pro spuštění

Při zadání hesla pro spuštění proveďte následující kroky:

1. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnosti **Start > Vypnout > Restartovat počítač.**
2. Jakmile se na obrazovce objeví ikona klíče, zadejte aktuální heslo a stiskněte klávesu **ENTER**.

Zadávejte znaky opatrně, z bezpečnostních důvodů se neobjevují na obrazovce.

Jestliže heslo nezadáte správně, zobrazí se ikona zlomeného klíče. Zadejte heslo znovu. Po třech neúspěšných pokusech musíte vypnout počítač, znovu ho zapnout a teprve potom můžete pokračovat.

Zadání hesla pro nastavení

Je-li systém vybaven zařízením Embedded Security, projděte si část „Embedded Security (Integrované zabezpečení) na stránce 30“.

Pokud bylo v počítači vytvořeno heslo pro nastavení, budete vyzváni k jeho zadání při každém spuštění nástroje Computer Setup.

1. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnosti **Start > Vypnout > Restartovat počítač.**
2. Jakmile se indikátor monitoru rozsvítí zeleně, stiskněte klávesu **F10**.

Jestliže klávesu **F10** nestisknete ve vhodné době, bude nutné počítač vypnout, znovu zapnout a znovu stisknout klávesu **F10**.

3. Jakmile se na obrazovce objeví ikona klíče, zadejte heslo pro nastavení a stiskněte klávesu **ENTER**.

Zadávejte znaky opatrně, z bezpečnostních důvodů se neobjevují na obrazovce.

Jestliže heslo nezadáte správně, zobrazí se ikona zlomeného klíče. Zadejte heslo znovu. Po třech neúspěšných pokusech musíte vypnout počítač, znovu ho zapnout a teprve potom můžete pokračovat.

Změna hesla pro spuštění nebo hesla pro nastavení

Je-li systém vybaven zařízením Embedded Security, projděte si část „Embedded Security (Integrované zabezpečení) na stránce 30“.

1. Spusťte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnosti **Start > Vypnout > Restartovat počítač**. Chcete-li změnit heslo pro nastavení, spusťte nástroj **Computer Setup**.
2. Po zobrazení ikony klíče zadejte aktuální heslo, lomítko (/) nebo alternativní oddělovací znak, nové heslo, další lomítko (/) nebo alternativní oddělovací znak a opět nové heslo:
   aktuální heslo/nové heslo/nové heslo

Zadávejte znaky opatrně, z bezpečnostních důvodů se neobjevují na obrazovce.

3. Stiskněte klávesu **ENTER**.

Nové heslo začne platit při příštím spuštění počítače.

Informace o alternativních oddělovacích znacích naleznete v části „Národní oddělovací znaky klávesnice na stránce 29“. Heslo pro spuštění a heslo pro nastavení lze změnit také pomocí příkazů nabídky Security (Zabezpečení) nástroje Computer Setup.

Odstranění hesla pro spuštění nebo hesla pro nastavení

Je-li systém vybaven zařízením Embedded Security, projděte si část „Embedded Security (Integrované zabezpečení) na stránce 30“.

1. Spusťte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnosti **Start > Vypnout > Restartovat počítač**. Chcete-li odstranit heslo pro nastavení, spusťte nástroj **Computer Setup**.
2. Jakmile se zobrazí ikona klíče, zadejte aktuální heslo a lomítko (/) nebo alternativní oddělovací znak:
   aktuální heslo/
3. Stiskněte klávesu **ENTER**.

Informace o alternativních oddělovacích znacích naleznete v části „Národní oddělovací znaky klávesnice“. Heslo pro spuštění a heslo pro nastavení lze změnit také pomocí příkazů nabídky Security (Zabezpečení) nástroje Computer Setup.

Národní oddělovací znaky klávesnice

Každá klávesnice je navržena tak, aby splňovala specifické požadavky dané země. Syntaxe a klávesy používané ke změně nebo odstranění hesla závisí na klávesnici dodávané s počítačem.

Národní oddělovací znaky klávesnice

arabština	/	řečtina	-	ruština	/
Belgie	=	hebrejština	.	slovenština	-
země bývalé Jugoslávie*	-	maďarština	-	španělština	-
Brazílie	/	italština	-	švédština a finština	/
čínština	/	japonština	/	Švýcarsko	-
čeština	-	korejština	/	Tchaj-wan	/
dánština	-	Latinská Amerika	-	thajština	/
francouzština	!	norština	-	turečtina	.
francouzština (Kanada)	é	polština	-	angličtina (Británie)	/
němčina	-	portugalština	-	angličtina (USA)	/

* Bosna a Hercegovina, Chorvatsko, Slovinsko a Jugoslávie

Vymazání hesel

Pokud zapomenete heslo, nebudete mít přístup k počítači. Pokyny k vymazání hesel naleznete v příručce *Poradce při potížích*.

Je-li systém vybaven zařízením Embedded Security, projděte si část „Embedded Security (Integrované zabezpečení)“.

Embedded Security (Integrované zabezpečení)

Funkce Embedded Security nástroje ProtectTools poskytuje kombinací šifrování a ochrany heslem rozšířené zabezpečení pro šifrování souborů nebo složek systému EFS (Embedded File System) a zabezpečený e-mail v aplikacích Microsoft Outlook a Outlook Express. Nástroj ProtectTools je k dispozici u vybraných stolních počítačů jako volitelná možnost na objednávku. Je určen pro zákazníky společnosti HP, pro něž jsou ohrožená data prvořadým zájmem: neoprávněný přístup k datům představuje mnohem větší nebezpečí než ztráta dat. V nástroji ProtectTools se používají čtyři hesla:

- (F10) Setup – Ke vstupu do nástroje Computer Setup (F10) a povolení nebo zakázání nástroje ProtectTools.
- Take Ownership (Převzít vlastnictví) – Nastavuje a používá správce, který bude udělovat práva uživatelům a nastavovat parametry zabezpečení.
- Emergency Recovery Token (Token nouzového obnovení) – Nastavuje správce systému, povoluje obnovení v případě selhání počítače nebo čipu nástroje ProtectTools.
- Basic User (Základní uživatel) – Nastavuje a používá koncový uživatel.

Pokud dojde ke ztrátě hesla koncového uživatele, nebude možné šifrovaná data obnovit. Nástroj ProtectTools je tedy bezpečné použít v případě, že jsou data disku uživatele zkopírována v informačním systému nebo jsou pravidelně zálohována.

Funkce Embedded Security nástroje ProtectTools je bezpečnostní čip kompatibilní s technologií TCPA 1.1 volitelně instalovaný na systémovou desku vybraných stolních počítačů. Každý čip Embedded Security nástroje ProtectTools je jedinečný a je vázán na specifický počítač. Každý čip provádí klíčové procesy zabezpečení nezávisle na jiných součástech počítače (například procesoru, paměti nebo operačním systému).

Počítač s funkcí ProtectTools Embedded Security doplňuje a rozšiřuje schopnosti zabezpečení, které jsou standardně k dispozici v systémech Microsoft Windows 2000 nebo Windows XP Professional nebo Home Edition. Operační systém může například šifrovat místní soubory a složky založené na systému EFS, avšak funkce ProtectTools Embedded Security nabízí další úroveň zabezpečení, protože vytváří šifrovací klíče z kořenového klíče platformy (který je uložen v silikonovém čipu). Tento proces se nazývá „zabalení“ (wrapping) šifrovacích klíčů. Nástroj ProtectTools nezabraňuje síťovému přístupu do počítače bez nástroje ProtectTools.

Mezi klíčové schopnosti funkce ProtectTools Embedded Security patří:

- ověřování platformy,
- chráněné úložiště dat,
- datová integrita.

UPOZORNĚNÍ: Uložte hesla na bezpečném místě. **Šifrovaná data nejsou bez hesel přístupná ani je nelze obnovit.**

Nastavení hesel

Nastavení

Lze vytvořit heslo pro nastavení (Setup) a pomocí nástroje pro nastavení F10 povolit zařízení integrovaného zabezpečení (Embedded Security).

1. Jakmile se indikátor monitoru rozsvítí zeleně, stiskněte klávesu **F10**.

Jestliže klávesu **F10** nestisknete ve vhodné době, bude nutné počítač vypnout, znovu zapnout a znovu stisknout klávesu **F10**.

2. Pomocí kláves se šipkami nahoru a dolů vyberte jazyk a potom stiskněte klávesu **ENTER**.
3. Klávesou se šipkou vpravo nebo vlevo přejděte na kartu **Security** (Zabezpečení) a klávesou se šipkou nahoru nebo dolů přejděte na položku **Setup Password** (Heslo pro nastavení). Stiskněte klávesu **ENTER**.

4. Zadejte a potvrďte heslo. Přijměte heslo klávesou **F10**.

Zadávejte znaky opatrně, z bezpečnostních důvodů se neobjevují na obrazovce.

5. Pomocí kláves se šipkami nahoru a dolů přejděte na položku **Embedded Security Device** (Zařízení integrovaného zabezpečení). Stiskněte klávesu **ENTER**.
6. Pokud je v dialogovém okně vybráno **Embedded Security Device–Disable** (Zakázat), změňte hodnotu klávesou vlevo nebo vpravo na **Embedded Security Device–Enable** (Povolit). Přijměte změnu klávesou **F10**.

UPOZORNĚNÍ: Pokud vyberete možnost **Reset to Factory Settings–Reset** (Obnovení továrních nastavení–Obnovit), budou všechny klíče vymazány a šifrovaná data budou obnovitelná *pouze* v případě, že byly klíče zálohovány (viz část „Funkce Take Ownership a Emergency Recovery Token“). Možnost **Reset** vyberte pouze v případě, kdy vám to určí pokyny v postupu obnovení šifrovaných dat (viz část „Obnovení šifrovaných dat na stránce 36“).

7. Pomocí kláves se šipkami vlevo a vpravo přejděte na položku **File** (Soubor). Pomocí kláves se šipkami nahoru a dolů přejděte na položku **Save Changes and Exit** (Uložit změny a ukončit program). Stiskněte klávesu **ENTER** a potvrďte klávesou **F10**.

Funkce Take Ownership a Emergency Recovery Token

Heslo Take Ownership je vyžadováno k povolení nebo zakázání bezpečnostní platformy a přidělování práv uživatelům. Pokud dojde k selhání zařízení integrovaného zabezpečení (Ebmedded Security), umožní mechanismus obnovení v nouzi (Emergency Recovery) přidávat práva uživatelům a přístup k datům.

1. Pokud používáte systém Windows XP Professional nebo Home Edition, klepněte na položky **Start > Všechny programy > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard** (Průvodce inicializací integrovaného zabezpečení).

Pokud používáte systém Windows 2000, klepněte na položky **Start > Programy > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard** (Průvodce inicializací integrovaného zabezpečení).

2. Klepněte na tlačítko **Next** (Další).
3. Zadejte a potvrďte heslo Take Ownership a klepněte na tlačítko **Next**.

Zadávejte znaky opatrně, z bezpečnostních důvodů se neobjevují na obrazovce.

4. Klepnutím na tlačítko **Next** přijměte výchozí umístění archivu obnovení.
5. Zadejte a potvrďte heslo Emergency Recovery Token (Token nouzového obnovení) a klepněte na tlačítko **Next**.
6. Vložte disketu, na kterou chcete uložit klíč Emergency Recovery Token. Klepněte na tlačítko **Browse** (Procházet) a vyberte disketu.

UPOZORNĚNÍ: Klíč Emergency Recovery Token slouží k obnovení šifrovaných dat v případě selhání počítače nebo čipu integrovaného zabezpečení. **Data nelze bez klíče obnovit.** (Bez hesla Basic User nejsou data ani přístupná.) Uložte disketu na bezpečném místě.

7. Klepnutím na tlačítko **Save** (Uložit) přijměte umístění a výchozí název souboru a pokračujte tlačítkem **Next**.
8. Klepnutím na tlačítko **Next** potvrďte nastavení před inicializací platformy zabezpečení.

Může dojít k zobrazení zprávy s textem, že funkce integrovaného zabezpečení (Embedded Security) nejsou inicializovány. Na tuto zprávu neklepejte. Záležitost bude vyřešena později a zpráva se za několik sekund zavře.

9. Klepnutím na tlačítko **Next** (Další) přeskočte konfigurování místních zásad.
10. Zkontrolujte, zda je zaškrtnuto políčko Start Embedded Security User Initialization Wizard (Spustit průvodce uživatelskou inicializací integrovaného zabezpečení), a klepněte na tlačítko **Finish** (Dokončit).

Průvodce bude automaticky spuštěn.

Basic User

Při inicializaci je vytvořeno heslo Basic User (Základní uživatel). Je vyžadováno k zadání šifrovaných dat a k přístupu k nim.

UPOZORNĚNÍ: Uložte heslo na bezpečném místě. **Šifrovaná data nejsou bez tohoto hesla přístupná ani je nelze obnovit.**

1. Pokud se průvodce neotevře:

   Jestliže používáte systém Windows XP Professional nebo Home Edition, klepněte na položky **Start > Všechny programy > HP ProtectTools Embedded Security Tools > User Initialization Wizard** (Průvodce inicializací uživatele).

   Jestliže používáte systém Windows 2000, klepněte na položky **Start > Programy > HP ProtectTools Embedded Security Tools > User Initialization Wizard** (Průvodce inicializací uživatele).

2. Klepněte na tlačítko **Next** (Další).
3. Zadejte a potvrďte heslo klíče Basic User a klepněte na tlačítko **Next**.

Zadávejte znaky opatrně, z bezpečnostních důvodů se neobjevují na obrazovce.

4. Klepnutím na tlačítko **Next** potvrďte nastavení.
5. Vyberte příslušné funkce zabezpečení a klepněte na tlačítko **Next**.
6. Klepnutím vyberte příslušný e-mailový klient a potom klepněte na tlačítko **Next**.
7. Klepnutím na tlačítko **Next** použijte šifrovací certifikát (Encryption Certificate).
8. Klepnutím na tlačítko **Next** potvrďte nastavení.
9. Klepněte na tlačítko **Finish** (Dokončit).
10. Restartujte počítač.

Obnovení šifrovaných dat

Chcete-li obnovit data po výměně čipu ProtectTools, musíte mít k dispozici tyto položky:

- soubor SPEmRecToken.xml – klíč Emergency Recovery Token,
- soubor SPEmRecArchive.xml – skrytá složka, výchozí umístění: C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive,
- hesla nástroje ProtectTools,
  - Setup (Nastavení),
  - Take Ownership (Převzít vlastnictví),
  - Emergency Recovery Token (Token nouzového obnovení),
  - Basic User (Základní uživatel).

1. Restartujte počítač.
2. Jakmile se indikátor monitoru rozsvítí zeleně, stiskněte klávesu **F10**.

Jestliže klávesu **F10** nestisknete ve vhodné době, bude nutné počítač vypnout, znovu zapnout a znovu stisknout klávesu **F10**.

3. Zadejte heslo pro nastavení a stiskněte klávesu **ENTER**.
4. Pomocí kláves se šipkami nahoru a dolů vyberte jazyk a potom stiskněte klávesu **ENTER**.
5. Klávesou se šipkou vpravo nebo vlevo přejděte na kartu **Security** (Zabezpečení) a klávesou se šipkou nahoru nebo dolů přejděte na položku **Embedded Security Device** (Zařízení integrovaného zabezpečení). Stiskněte klávesu **ENTER**.
6. Je-li k dispozici pouze jedna hodnota, **Embedded Security Device – Disable** (Zakázat):
   a. Pomocí kláves se šipkami vlevo a vpravo ji změňte na hodnotu **Embedded Security Device – Enable** (Povolit). Přijměte změnu klávesou **F10**.

b. Pomocí kláves se šipkami vlevo a vpravo přejděte na položku **File** (Soubor). Pomocí kláves se šipkami nahoru a dolů přejděte na položku **Save Changes and Exit** (Uložit změny a ukončit program). Stiskněte klávesu **ENTER** a potvrďte klávesou **F10**.

c. Přejděte ke kroku 1.

Jsou-li na výběr dvě možnosti, přejděte ke kroku 7.

7. Pomocí kláves se šipkami nahoru a dolů přejděte na položku **Reset to Factory Settings – Do Not Reset** (Obnovit tovární nastavení – Neobnovovat). Stiskněte jednou klávesu se šipkou vlevo nebo vpravo.

   Zobrazí se zpráva: Pokud budou nastavení při ukončení programu uložena, obnoví tato akce v zařízení integrovaného zabezpečení tovární nastavení. Pokračujte stisknutím libovolné klávesy.

   Stiskněte klávesu **ENTER**.

8. Nyní bude vybraná možnost **Reset to Factory Settings – Reset** (Obnovit tovární nastavení – Obnovit). Přijměte změnu klávesou **F10**.

9. Pomocí kláves se šipkami vlevo a vpravo přejděte na položku **File** (Soubor). Pomocí kláves se šipkami nahoru a dolů přejděte na položku **Save Changes and Exit** (Uložit změny a ukončit program). Stiskněte klávesu **ENTER** a potvrďte klávesou **F10**.

10. Restartujte počítač.

11. Jakmile se indikátor monitoru rozsvítí zeleně, stiskněte klávesu **F10**.

Jestliže klávesu **F10** nestisknete ve vhodné době, bude nutné počítač vypnout, znovu zapnout a znovu stisknout klávesu **F10**.

12. Zadejte heslo pro nastavení a stiskněte klávesu **ENTER**.

13. Pomocí kláves se šipkami nahoru a dolů vyberte jazyk a potom stiskněte klávesu **ENTER**.

14. Klávesou se šipkou vpravo nebo vlevo přejděte na kartu **Security** (Zabezpečení) a klávesou se šipkou nahoru nebo dolů přejděte na položku **Embedded Security Device** (Zařízení integrovaného zabezpečení). Stiskněte klávesu **ENTER**.

15. Pokud je v dialogovém okně vybráno **Embedded Security Device – Disable** (Zakázat), změňte hodnotu klávesou vlevo nebo vpravo na **Embedded Security Device – Enable** (Povolit). Stiskněte klávesu **F10**.
16. Pomocí kláves se šipkami vlevo a vpravo přejděte na položku **File** (Soubor). Pomocí kláves se šipkami nahoru a dolů přejděte na položku **Save Changes and Exit** (Uložit změny a ukončit program). Stiskněte klávesu **ENTER** a potvrďte klávesou **F10**.
17. Po spuštění systému Windows:

    Pokud používáte systém Windows XP Professional nebo Home Edition, klepněte na položky **Start > Všechny programy > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard** (Průvodce inicializací integrovaného zabezpečení).

    Pokud používáte systém Windows 2000, klepněte na položky **Start > Programy > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard** (Průvodce inicializací integrovaného zabezpečení).
18. Klepněte na tlačítko **Next** (Další).
19. Zadejte a potvrďte heslo převzetí vlastnictví (Take Ownership). Klepněte na tlačítko **Next** (Další).

Zadávejte znaky opatrně, z bezpečnostních důvodů se neobjevují na obrazovce.

20. Ověřte, zda je vybrána položka Create a new recovery archive (Vytvořit nový archiv obnovení). V části **Recovery archive location** (Umístění archivu obnovení) klepněte na tlačítko **Browse** (Procházet).
21. Nepřijímejte výchozí název souboru. Zadejte nový název, abyste nepřepsali původní soubor.
22. Klepněte na tlačítko **Save** (Uložit) a potom na tlačítko **Next** (Další).
23. Zadejte a potvrďte heslo Emergency Recovery Token (Token nouzového obnovení) a klepněte na tlačítko **Next**.
24. Vložte disketu, na kterou chcete uložit klíč Emergency Recovery Token. Klepněte na tlačítko **Browse** (Procházet) a vyberte disketu.
25. Nepřijímejte výchozí název klíče. Zadejte nový název, abyste nepřepsali původní klíč.

26. Klepněte na tlačítko **Save** (Uložit) a potom na tlačítko **Next** (Další).
27. Klepnutím na tlačítko **Next** potvrďte nastavení před inicializací platformy zabezpečení.

Může dojít k zobrazení zprávy s textem, že klíč Basic User nelze zavést. Na tuto zprávu neklepejte. Záležitost bude vyřešena později a zpráva se za několik sekund zavře.

28. Klepnutím na tlačítko **Next** (Další) přeskočte konfigurování místních zásad.
29. Klepnutím zrušte zaškrtnutí políčka **Start Embedded Security User Initialization Wizard** (Spustit průvodce uživatelskou inicializací integrovaného zabezpečení). Klepněte na tlačítko **Finish** (Dokončit).
30. Klepněte pravým tlačítkem myši na ikonu ProtectTools na panelu nástrojů a klepněte na příkaz **Initialize Embedded Security restoration** (Inicializovat obnovení integrovaného zabezpečení).

    Bude spuštěn průvodce HP ProtectTools Embedded Security Initialization Wizard.
31. Klepněte na tlačítko **Next** (Další).
32. Vložte disketu, na které je uložen původní klíč Emergency Recovery Token. Klepněte na tlačítko **Browse** (Procházet), vyhledejte token a po poklepání na něj zadejte název. Výchozí možnost je A:\SPEmRecToken.xml.
33. Zadejte původní heslo tokenu a klepněte na tlačítko **OK**.
34. Klepněte na tlačítko **Browse** (Procházet), vyhledejte původní archiv obnovení a po poklepání na něj zadejte název. Výchozí možnost je C:\Documents and Settings\All Users\Application Data \Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml.
35. Klepněte na tlačítko **Next** (Další).
36. Klepněte na počítač, který chcete obnovit, a klepněte na tlačítko **Next** (Další).
37. Klepnutím na tlačítko **Next** nastavení potvrďte.

38. Pokud průvodce oznámí, že platforma zabezpečení byla obnovena, přejděte ke kroku 39.

    Pokud průvodce oznámí, že se obnovení nezdařilo, vraťte se ke kroku 10. Důkladně zkontrolujte hesla, umístění a název tokenu a umístění a název archivu.

39. Klepněte na tlačítko Finish (Dokončit).

40. Jestliže používáte systém Windows XP Professional nebo Home Edition, klepněte na položky **Start > Všechny programy > HP ProtectTools Embedded Security Tools > User Initialization Wizard** (Průvodce inicializací uživatele).

    Jestliže používáte systém Windows 2000, klepněte na položky **Start > Programy > HP ProtectTools Embedded Security Tools > User Initialization Wizard** (Průvodce inicializací uživatele).

41. Klepněte na tlačítko **Next** (Další).

42. Klepněte na možnost **Recover your basic user key** (Obnovit klíč základního uživatele) a pokračujte tlačítkem **Next**.

43. Vyberte uživatele, zadejte původní heslo klíče Basic User tohoto uživatele a klepněte na tlačítko **Next** (Další).

44. Klepnutím na tlačítko **Next** potvrďte nastavení a přijměte výchozí umístění dat obnovení.

Kroky 45 až 49 znovu nainstalují původní konfiguraci Basic User.

45. Vyberte příslušné funkce zabezpečení a klepněte na tlačítko **Next**.

46. Klepnutím vyberte příslušný e-mailový klient a potom klepněte na tlačítko **Next**.

47. Klepněte na možnost Encryption Certificate (Šifrovací certifikát) a klepnutím na tlačítko **Next** (Další) jej použijte.

48. Klepnutím na tlačítko **Next** potvrďte nastavení.

49. Klepněte na tlačítko **Finish** (Dokončit).

50. Restartujte počítač.

UPOZORNĚNÍ: Uložte heslo na bezpečném místě. **Šifrovaná data nejsou bez tohoto hesla přístupná ani je nelze obnovit.**

DriveLock

Funkce DriveLock představuje standardní zabezpečení před neoprávněným přístupem k datům na pevných discích v multifunkční pozici. Byla implementována jako rozšíření nástroje Computer Setup. Je k dispozici pouze v případě, že byly zjištěny pevné disky, které lze testovat pomocí funkce DriveLock.

Funkce DriveLock je určena pro zákazníky společnosti HP, pro něž je zabezpečení dat prvořadou záležitostí. Pro takové zákazníky je cena pevného disku a ztráta na něm uložených dat zanedbatelná ve srovnání se škodami, které mohou vzniknout v důsledku neoprávněného přístupu k datům. V zájmu zachování požadované úrovně zabezpečení a současně praktické potřeby zjistit zapomenuté heslo využívá tato implementace funkce DriveLock schéma zabezpečení se dvěma hesly. Jedno heslo nastavuje a používá správce systému. Druhé heslo je obvykle nastavováno a používáno koncovým uživatelem. Pokud byla zapomenuta obě hesla, neexistuje žádná možnost, jak jednotku odemknout. Proto je nejvhodnější používat funkci DriveLock v případě, že data pevného disku jsou replikována v podnikovém informačním systému nebo jsou pravidelně zálohována.

Dojde-li ke ztrátě obou hesel funkce DriveLock, je pevný disk trvale nepoužitelný. Pro uživatele, kteří neodpovídají výše uvedenému profilu, může tato skutečnost představovat nepřijatelné riziko. Pro uživatele, kteří tomuto profilu vyhovují, se vzhledem k povaze dat uložených na pevném disku může jednat o riziko přijatelné.

Použití funkce DriveLock

Možnost DriveLock je součástí nabídky Security (Zabezpečení) nástroje Computer Setup. K dispozici jsou možnosti pro nastavení hlavního hesla nebo povolení funkce DriveLock. K povolení funkce DriveLock je nezbytné zadat uživatelské heslo. Počáteční konfiguraci funkce DriveLock provádí obvykle správce systému. Z tohoto důvodu musí být nejdříve nastaveno hlavní heslo. Společnost HP doporučuje správcům systému, aby hlavní heslo nastavili bez ohledu na to, zda mají v úmyslu funkci DriveLock povolit či zakázat. Získají tak možnost upravit nastavení funkce DriveLock v případě, že v budoucnu dojde k uzamčení jednotky. Po nastavení hlavního hesla může správce systému funkci DriveLock povolit nebo zakázat.

Je-li zjištěna uzamčená jednotka pevného disku, bude test POST vyžadovat k odemknutí zařízení heslo. Pokud se nastavené heslo pro spuštění shoduje s uživatelským heslem zařízení, uživatel nebude testem POST vyzván k jeho opětovnému zadání. V opačném případě se zobrazí výzva k zadání hesla funkce DriveLock. Může být použito hlavní i uživatelské heslo. Uživatelé mají dva pokusy k zadání správného hesla. Nebude-li ani jeden z pokusů úspěšný, test POST bude pokračovat, avšak jednotka zůstane nepřístupná.

Použití funkce DriveLock

Zabezpečovací funkci DriveLock lze nejvhodněji využít v podnikovém prostředí, ve kterém správce systému poskytuje uživatelům některých počítačů pevné disky pro multifunkční pozici. Správce systému zodpovídá za konfiguraci pevného disku pro multifunkční pozici, což mimo jiné zahrnuje i nastavení hlavního hesla funkce DriveLock. V případě, že uživatel heslo zapomene nebo zařízení převezme jiný zaměstnanec, může být hlavní heslo vždy využito k novému nastavení uživatelského hesla a obnovení přístupu k jednotce pevného disku.

Společnost HP doporučuje správcům systému, kteří se rozhodnou funkci DriveLock povolit, aby rovněž vytvořili podnikové zásady pro nastavení a údržbu hlavních hesel. Tím by se mělo zabránit situaci, kdy zaměstnanec úmyslně či neúmyslně nastaví obě hesla funkce DriveLock a poté podnik opustí. V takovém případě by se stal pevný disk nepoužitelným a bylo by nutné jej vyměnit. Podobně by se mohlo stát, že by vinou nenastavení hlavního hesla byl správcům systému odepřen přístup k jednotce pevného disku. Nemohli by pak provádět běžná zjišťování neoprávněného softwaru, používat ostatních funkce řízení inventárních čísel ani poskytovat podporu.

Společnost HP nedoporučuje použití funkce DriveLock u uživatelů s méně přísnými požadavky na zabezpečení. Do této kategorie spadají soukromí uživatelé nebo uživatelé, kteří na pevných discích neuchovávají citlivá data. U takových uživatelů riziko možné ztráty pevného disku vinou zapomenutí obou hesel značně převyšuje hodnotu dat, k jejichž ochraně byla funkce DriveLock vytvořena. Přístup k nástroji Computer Setup a funkci DriveLock může být omezen prostřednictvím hesla pro nastavení. Pokud správce určí heslo pro nastavení a neposkytne je koncovým uživatelům, může jim přístup k funkci DriveLock omezit.

Senzor zámku počítačové skříně

Senzor zámku počítačové skříně, který je k dispozici u vybraných modelů, představuje kombinaci hardwarových a softwarových technologií. Upozorní uživatele při sejmutí krytu nebo bočního panelu počítače. Existují tři úrovně ochrany, které jsou popsány v následující tabulce.

Úrovně ochrany senzorem zámku počítačové skříně

Úroveň	Nastavení	Popis
Úroveň 0	Disabled (Vypnuto)	Senzor zámku počítačové skříně je vypnut (výchozí nastavení).
Úroveň 1	Notify user (Upozornit uživatele)	Po restartování počítače se na obrazovce zobrazí zpráva oznamující sejmutí krytu nebo bočního panelu počítače.
Úroveň 2	Setup Password (Heslo pro nastavení)	Po restartování počítače se na obrazovce zobrazí zpráva oznamující sejmutí krytu nebo bočního panelu počítače. Pokud chcete pokračovat, musíte zadat heslo pro nastavení.

✎ Toto nastavení lze zmìnit pomocí nástroje Computer Setup. Další informace o nástroji Computer Setup naleznete v *Příručce k nástroji Computer Setup (F10).*

Nastavení úrovně ochrany senzorem zámku počítačové skříně

Chcete-li nastavit úroveň ochrany senzorem zámku počítačové skříně, proveďte následující kroky:

1. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnosti **Start > Vypnout > Restartovat počítač**.
2. Jakmile se indikátor monitoru rozsvítí zeleně, stiskněte klávesu **F10**. V případě potřeby můžete stisknutím klávesy **ENTER** přeskočit úvodní obrazovku.

Jestliže klávesu **F10** nestisknete ve vhodné době, bude nutné počítač vypnout, znovu zapnout a znovu stisknout klávesu **F10**.

3. V nabídce **Security** (Zabezpečení) vyberte příkaz **Smart Cover** (Zámek a senzor počítačové skříně) a postupujte podle pokynů na obrazovce.
4. Před ukončením práce zvolte možnosti **File (Soubor) > Save Changes and Exit (Uložit změny a ukončit program)**.

Zámek počítačové skříně (Smart Cover Lock)

Zámek počítačové skříně je ovládán prostřednictvím softwaru a jsou jím vybaveny vybrané počítače společnosti HP. Tento zámek zabraňuje neoprávněnému přístupu k interním součástem počítače. Počítače jsou dodávány se zámkem počítačové skříně v odemknuté pozici.

UPOZORNĚNÍ: Chcete-li zajistit maximální zabezpečení zámku počítačové skříně, vytvořte heslo pro nastavení. Heslo pro nastavení zabraňuje neoprávněnému přístupu k nástroji Computer Setup.

Zámek počítačové skříně je volitelná funkce, která je k dispozici u vybraných modelů.

Uzamčení zámku počítačové skříně

Chcete-li zámek počítačové skříně aktivovat a uzamknout, proveďte následující kroky:

1. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnosti **Start > Vypnout > Restartovat počítač**.
2. Jakmile se indikátor monitoru rozsvítí zeleně, stiskněte klávesu **F10**. V případě potřeby můžete stisknutím klávesy **ENTER** přeskočit úvodní obrazovku.

Jestliže klávesu **F10** nestisknete ve vhodné době, bude nutné počítač vypnout, znovu zapnout a znovu stisknout klávesu **F10**.

3. V nabídce **Security** (Zabezpečení) vyberte příkaz **Smart Cover** (Zámek a senzor počítačové skříně) a potom vyberte možnost **Locked** (Uzamknuto).
4. Před ukončením práce zvolte možnosti **File (Soubor) > Save Changes and Exit (Uložit změny a ukončit program)**.

Odemknutí zámku počítačové skříně

1. Spusťte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnosti **Start > Vypnout > Restartovat počítač**.
2. Jakmile se indikátor monitoru rozsvítí zeleně, stiskněte klávesu **F10**. V případě potřeby můžete stisknutím klávesy **ENTER** přeskočit úvodní obrazovku.

Jestliže klávesu **F10** nestisknete ve vhodné době, bude nutné počítač vypnout, znovu zapnout a znovu stisknout klávesu **F10**.

3. Zvolte možnosti **Security (Zabezpečení) > Smart Cover (Zámek a senzor počítačové skříně) > Unlocked (Odemknuto)**.
4. Před ukončením práce zvolte možnosti **File (Soubor) > Save Changes and Exit (Uložit změny a ukončit program)**.

Použití bezpečnostního klíče (Smart Cover FailSafe Key)

Je-li zapnutý zámek počítačové skříně a nemůžete zadat heslo, které by jej odemknulo, budete k otevření krytu počítače potřebovat bezpečnostní klíč. Tento klíč je nutné použít, nastane-li některá z následujících situací:

- výpadek napájení,
- selhání při spuštění,
- selhání některé součásti počítače (například procesoru nebo zdroje),
- zapomenutí hesla.

UPOZORNĚNÍ: Bezpečnostní klíč je speciální nástroj, který můžete získat od společnosti HP. Připravte se proto předem a objednejte si tento klíč dříve, než jej budete potřebovat, a to u autorizovaného prodejce nebo poskytovatele služeb.

Bezpečnostní klíč můžete získat některým z následujících způsobů:

- Obraťte se na autorizovaného prodejce nebo poskytovatele služeb společnosti HP.
- Zavolejte na příslušné telefonní číslo uvedené v záruční smlouvě.

Další informace o použití bezpečnostního klíče naleznete v *Referenční příručce k hardwaru*.

Master Boot Record Security (Hlavní spouštěcí záznam)

Hlavní spouštěcí záznam obsahuje informace potřebné k úspěšnému spuštění z disku a k přístupu k datům uloženým na disku. Zabezpečením hlavního spouštěcího záznamu můžete předejít neúmyslným změnám nebo záměrnému poškození hlavního spouštěcího záznamu, k čemuž může dojít vinou některých počítačových virů nebo nesprávným použitím určitých nástrojů pro práci s disky. Umožňuje také obnovit poslední známý platný hlavní spouštěcí záznam, pokud jsou při restartování systému v tomto záznamu zjištěny změny.

Chcete-li povolit zabezpečení hlavního spouštěcího záznamu, proveďte následující kroky:

1. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnosti **Start > Vypnout > Restartovat počítač**.
2. Jakmile se indikátor monitoru rozsvítí zeleně, stiskněte klávesu **F10**. V případě potřeby můžete stisknutím klávesy **ENTER** přeskočit úvodní obrazovku.

Jestliže klávesu **F10** nestisknete ve vhodné době, bude nutné počítač vypnout, znovu zapnout a znovu stisknout klávesu **F10**.

3. Zvolte možnosti **Security (Zabezpečení) > Master Boot Record Security (Zabezpečení hlavního spouštěcího záznamu) > Enabled (Povoleno)**.
4. Zvolte možnosti **Security (Zabezpečení) > Save Master Boot Record (Uložit hlavní spouštěcí záznam)**.
5. Před ukončením práce zvolte možnosti **File (Soubor) > Save Changes and Exit (Uložit změny a ukončit program)**.

Jestliže je funkce zabezpečení hlavního spouštěcího záznamu zapnuta, zabraňuje systém BIOS jakýmkoli změnám v hlavním spouštěcím záznamu aktuálního spouštěcího disku v systému MS-DOS nebo nouzovém režimu systému Windows.

Většina operačních systémů řídí přístup k hlavnímu spouštěcímu záznamu aktuálního spouštěcího disku. Systém BIOS nedokáže předejít změnám, ke kterým může dojít v průběhu činnosti operačního systému.

Při každém spuštění nebo restartování počítače porovná systém BIOS hlavní spouštěcí záznam aktuálního spouštěcího disku s uloženým hlavním spouštěcím záznamem. Jsou-li zjištěny změny a je-li aktuálním spouštěcím diskem disk, ze kterého byl uložen hlavní spouštěcí záznam, zobrazí se následující zpráva:

1999 - Master Boot Record has changed (1999 – Došlo ke změně hlavního spouštěcího záznamu.)

Stisknutím libovolné klávesy spusťte program Setup ke konfiguraci zabezpečení hlavního spouštěcího záznamu.

Po spuštění nástroje Computer Setup je nutné provést tyto akce:

- Uložte hlavní spouštěcí záznam aktuálního spouštěcího disku
- Obnovte uložený hlavní spouštěcí záznam. (nebo)
- Zakažte funkci zabezpečení hlavního spouštěcího záznamu.

Jestliže existuje heslo pro nastavení, bude třeba jej zadat.

Jsou-li zjištěny změny a aktuálním spouštěcím diskem **není** disk, ze kterého byl uložen hlavní spouštěcí záznam, zobrazí se následující zpráva:

2000 - Master Boot Record Hard Drive has changed (2000 – Došlo ke změně hlavního spouštěcího záznamu jednotky pevného disku.)

Stisknutím libovolné klávesy spusťte program Setup ke konfiguraci zabezpečení hlavního spouštěcího záznamu.

Po spuštění nástroje Computer Setup je nutné provést tyto akce:

- Uložte hlavní spouštěcí záznam aktuálního spouštěcího disku. (nebo)
- Zakažte funkci zabezpečení hlavního spouštěcího záznamu.

Jestliže existuje heslo pro nastavení, bude třeba jej zadat.

Ve velmi nepravděpodobném případě poškození právě uloženého hlavního spouštěcího záznamu se zobrazí následující zpráva:

1998 - Master Boot Record has been lost (1998 – Došlo ke ztrátě hlavního spouštěcího záznamu.)

Stisknutím libovolné klávesy spusťte program Setup ke konfiguraci zabezpečení hlavního spouštěcího záznamu.

Po spuštění nástroje Computer Setup je nutné provést tyto akce:

- Uložte hlavní spouštěcí záznam aktuálního spouštěcího disku. (nebo)
- Zakažte funkci zabezpečení hlavního spouštěcího záznamu.

Jestliže existuje heslo pro nastavení, bude třeba jej zadat.

Před rozdělením nebo naformátováním aktuálního spouštěcího disku

Před prováděním změn v rozdělení nebo formátování aktuálního spouštěcího disku se ujistěte, že zabezpečení hlavního spouštěcího záznamu bylo zakázáno. Některé nástroje pro práci s disky (například FDISK nebo FORMAT) se pokoušejí hlavní spouštěcí záznam aktualizovat. Pokud byla funkce zabezpečení hlavního spouštěcího záznamu při změně rozdělení nebo formátování povolena, mohou se při příštím zapnutí nebo restartování počítače zobrazit chybové zprávy nástrojů pro práci s disky nebo varování funkce zabezpečení hlavního spouštěcího záznamu. Chcete-li funkci zabezpečení hlavního spouštěcího záznamu zakázat, proveďte následující kroky:

1. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnosti **Start > Vypnout > Restartovat počítač**.
2. Jakmile se indikátor monitoru rozsvítí zeleně, stiskněte klávesu **F10**. V případě potřeby můžete stisknutím klávesy **ENTER** přeskočit úvodní obrazovku.

Jestliže klávesu **F10** nestisknete ve vhodné době, bude nutné počítač vypnout, znovu zapnout a znovu stisknout klávesu **F10**.

3. Zvolte možnosti **Security (Zabezpečení) > Master Boot Record Security (Zabezpečení hlavního spouštěcího záznamu) > Disabled (Zakázáno)**.
4. Před ukončením práce zvolte možnosti **File (Soubor) > Save Changes and Exit (Uložit změny a ukončit program)**.

Zajištění pro lankový zámek

Zadní panel počítače je přizpůsoben pro použití lankového zámku, který umožňuje počítač fyzicky připevnit k pracovnímu místu.

Obrázky s pokyny naleznete v *Referenční příručce k hardwaru* na disku CD-ROM *Knihovna dokumentace*.

Technologie identifikace pomocí otisku prstů

Technologie identifikace pomocí otisku prstů společnosti HP odstraňuje nutnost zadávání hesel, čímž zlepšuje zabezpečení sítě, zjednodušuje proces přihlášení a omezuje náklady spojené se správou podnikových sítí. Tato cenově dostupná technologie již není určena pouze pro supermoderní vysoce zabezpečené organizace.

Podpora technologie identifikace pomocí otisku prstů se u jednotlivých modelů liší.

Další informace naleznete na adrese http://h18000.www1.hp.com/solutions/security.

Zobrazení informací o selhání systému a jeho obnovení

Funkce zobrazení informací o selhání systému a jeho obnovení spojuje nové hardwarové a softwarové technologie s cílem zabránit ztrátě důležitých dat a minimalizovat neplánované prostoje.

Pokud dojde k selhání, zobrazí se upozornění Local Alert obsahující popis selhání a případné doporučené akce. Pomocí nástroje HP Client Manager můžete zobrazit aktuální stav systému. Jestliže je počítač připojen k síti spravované pomocí nástroje HP Insight Manager, HP Client Manager nebo jiné aplikace pro správu systému, odešle počítač informace o selhání systému také aplikaci pro správu sítě.

Nástroj Drive Protection System

Nástroj DPS (Drive Protection System) je diagnostický nástroj, který je součástí pevných disků nainstalovaných ve vybraných modelech počítačů HP. Nástroj DPS je navržen tak, aby usnadňoval diagnostiku problémů, které by mohly vést k výměně pevného disku, na kterou se nevztahuje záruka.

Během výroby počítačů HP jsou všechny instalované pevné disky testovány nástrojem DPS a získané klíčové informace jsou zapsány na pevný disk. Výsledky testů jsou na pevný disk zapsány při každém spuštění nástroje DPS. Poskytovatel služeb může tyto informace použít ke zjištění okolností, za kterých bylo nutné spustit software DPS. Pokyny k použití nástroje DPS naleznete v příručce *Poradce při potížích*.

Napájecí zdroj s ochranou proti přepětí

Integrovaný napájecí zdroj s ochranou proti přepětí poskytuje větší spolehlivost, pokud je počítač zasažen nepředvídatelným přepětím v napájecí síti. Tento napájecí zdroj vydrží přepětí až 2 000 V, aniž by došlo k prostojům či ztrátě dat.

Tepelné čidlo

Tepelné čidlo je hardwarová a softwarová funkce, která sleduje vnitřní teplotu počítače. Při překročení normálního rozsahu zobrazí tato funkce varovné hlášení, které uživateli poskytne čas k přijetí opatření dříve, než dojde k poškození vnitřních součástí nebo ztrátě dat.

Rejstřík

S

T

Ú

U

V

W

Z